UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/841,503	04/24/2001	Richard Alan Dayan	RPS9 2001 0011	5669

53493 7590 03/09/2011

LENOVO (US) IP Law
1009 Think Place
Building One, 4th Floor 4B6
Morrisville, NC 27560

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2491	

MAIL DATE	DELIVERY MODE
03/09/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte RICHARD ALAN DAYAN, JOSEPH WAYNE FREEMAN,
WILLIAM FRED JR. KEOWN, and RANDALL SCOTT SPINGFIELD

Appeal 2009-005557
Application 09/841,503
Technology Center 2400

Before: LANCE LEONARD BARRY, HOWARD B. BLANKENSHIP, and JAMES R. HUGHES, *Administrative Patent Judges*.

BARRY, *Administrative Patent Judge*.

DECISION ON APPEAL[1]

---

[1] The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the "MAIL DATE" (paper delivery mode) or the "NOTIFICATION DATE" (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

STATEMENT OF THE CASE

The Patent Examiner rejected claims 44-49 and 57-62. The Appellants appeal therefrom under 35 U.S.C. § 134(a). We have jurisdiction under 35 U.S.C. § 6(b).

INVENTION

The Appellants describe the invention at issue on appeal as follows.

> A computer system includes a hard drive having a protected partition, which is locked during operation of an initialization program following power on in the system. A trusted server generates an update partition file, which is transferred to the computer system to be stored in non-volatile storage. During subsequent initialization, before the protected partition is locked, encrypted information available only to the server and the computer system is used to verify that the file was generated by the server, and the file is used to update information within the protected partition.

(Abstract.)

ILLUSTRATIVE CLAIM

57. An interconnected system for providing updated information in a secure manner, wherein

the interconnected system comprises a network, server system connected to the network and programmed to generate an update partition file and to transmit the update partition file over the network; and a computer system connected to the network,

the computer system includes a processor, non-volatile data storage including a hard drive having a protected partition,

the processor is programmed to receive the update partition file from the network and to store the update partition file in a predetermined location within the nonvolatile data storage outside the protected partition,

the nonvolatile data storage stores an operating system and an initialization routine, executing within the processor after power on of the computer system, including instructions causing the protected partition to be locked before the operating system is loaded, and the instruction causing information stored within the predetermined location to be written within the protected partition after predetermined security procedures have occurred but before the protected partition is locked,

the initialization routine includes instructions causing the processor of the computer system to perform a method including:

comparing information stored in the protected partition with information from the update partition file stored within the predetermined location;

when a portion of the information stored in the protected partition is found to match a portion of the information stored within the update partition file, overwriting the portion of the information stored in the protected partition with the portion of the information stored in the protected partition if space around the portion of the information stored in the protected partition is sufficient;

when a portion of the information stored in the protected partition is not found to match a portion of the information stored within the update partition file, writing the portion of the information stored within the update partition file to append to the information stored in the protected partition if space within the protected partition is sufficient; and

locking the protected partition to prevent further modification of information stored within the protected partition;

the update partition file includes a plurality of entries and a plurality of encrypted elements,

each entry within the plurality of entries includes information to be stored at a different location within the protected partition,

each encrypted element within the plurality of encrypted elements is associated with an entry in the plurality of entries.

the method additionally comprises, following determining that the update partition file is stored within the computing system for updating the protected partition, verifying whether each entry in the plurality of entries within the update partition file has been generated by the server system, and

each entry in the plurality of entries within the update partition file is written to the protected partition only following verification that the entry has been generated by the server system.

REFERENCES AND REJECTIONS

Menezes et al., *Handbook of Applied Cryptography*, CRC Press 1997.

Arnold	US 5,128,995	Jul. 7, 1992
Schmidt	US 5,826,015	Oct. 20, 1998
Gafken	US 6,026,016	Feb. 15, 2000
Hasbun	US 6,088,759	Jul. 11, 2000
Hayashi	US 2001/0039651 A1	Nov. 8, 2001

Claims 44-48 and 57-61 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Gafken, Arnold, Hasbun, Hayashi, and Menezes.

Claims 49 and 62 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Gafken, Arnold, Hasbun, Hayashi, Schmidt, and Menezes.

ISSUES

Based on the Appellants' arguments, we will decide the appeal of claims 44-48 and 57-61 on the basis of claim 57 alone. *See* 37 C.F.R. § 41.37(c)(1)(vii). The *issues* before us are whether the Examiner erred in finding that (1) the combined teachings of Gafken and Hayashi would have suggested an update file that includes a plurality of entries and a plurality of encrypted elements, wherein each encrypted element is associated with an entry, and verifying whether each entry has been generated by a server system, as required by representative claim 57, and (2) the combined teachings of Gafken, Arnold, Hasbun, Hayashi, Schmidt, and Menezes would have suggested the limitations of claims 49 and 62.

FINDINGS OF FACT

Gafken describes its invention as "locking and unlocking blocks of memory cells in a nonvolatile memory device to disable and enable write and erase, and in some cases, read operations to the blocks of memory." (Col. 1, ll. 7-10.)

Hayashi describes its invention as "translating information such as source files encoded to protect the security of the information." (¶ 0002.)

ANALYSIS

We address the aforementioned issues *seriatim.*

CLAIMS 44-48 AND 57-61

The question of obviousness is "based on underlying factual determinations including . . . what th[e] prior art teaches explicitly and inherently . . . ." *In re Zurko*, 258 F.3d 1379, 1383 (Fed. Cir. 2001) (citations omitted). "The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art." *In re Young*, 927 F.2d 588, 591 (Fed. Cir. 1991) (citing *In re Keller*, 642 F.2d 413, 425 (CCPA 1981)).

Here, the Examiner bases the rejection on the combined teachings of Gafken and Hayashi *inter alia.* More, specifically, he makes the following findings.

> Gafken, in Col. 12 Line 53 - Col. 13 Line 2, disclosed a code image with a code image signature for updating a BIOS [i.e., basic input/output system], which is equivalent to the update partition file of the claim language . . . .

> With regards to the plurality of entries, Hasbun renders obvious that in a BIOS update, the update data can be divided into blocks. These blocks read on the plurality of entries.
>
> . . . .
>
> Furthermore, the teachings of Hayashi suggest that in software updating, blocks of the update data should be encrypted separately in order to relieve the burden on the update servers. As such, one of ordinary skill in the art would have found it obvious to sign (calculate a digest and encrypt) each block of the code image of Gafken and Hasbun separately, thereby creating an alternative plurality of encrypted elements.
>
> As such, it can be seen that the limitation of the update partition file including a plurality of entries and a plurality of encrypted elements has been met by the combination of prior art references.
>
> Regarding the limitation that "wherein each encrypted element in the plurality of encrypted elements is associated with an entry in the plurality of entries", the examiner believes that the combination of references relied upon meets this limitation. . . . . [Specifically,] a separate signature is calculated for each block, each signature is associated with the block (entry) from which it was calculated.
>
> Regarding the limitation that "wherein the method performed by the initialization program includes verifying whether each entry in the plurality of entries has been generated by the server system", the examiner believes that this limitation is met by the combination of applied references. Gafken clearly disclosed verifying that the code image was generated by the server system, as can be seen in Gafken Col. 12 Line 53 - Col. 13 Line 2. . . . [Specifically,] wherein a separate, signature was calculated for each block (entry) of the code image, in order to verify the [whole] code image as disclosed by Gafken, the signature of each block would need to be verified.

(Ans. 17-19.)

"Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references." *In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) (citing *Keller*, 642 F.2d at 425). In determining obviousness, furthermore, a reference "must be read, not in isolation, but for what it fairly teaches in combination with the prior art as a whole." *Id.*

Here, the Appellants argue that "[t]here is no indication within *Gafken* that a separate validation process performed for each of multiple entries within the code image; the entire image is validated as a whole." (Appeal Br. 13-14.) They add the following arguments.

> *Hayashi et al.* merely describes a file including differently encrypted entries, not a file containing a plurality of entries and a plurality of encrypted elements, with each of the encrypted elements associated with one of the entries . . . . In addition, . . . *Hayashi et al.* does not describe a process for verifying that individual portions of the stored data . . . .

(*Id.* at 14.)

Because the rejection is based upon the combined teachings of Gafken and Hayashi *inter alia,* such arguments about the references individually cannot establish non-obviousness. Therefore, we *conclude* that the Examiner did not err in finding that the combined teachings of Gafken and Hayashi would have suggested an update file that includes a plurality of entries and a plurality of encrypted elements, wherein each encrypted element is associated with an entry, and verifying whether each entry has been generated by a server system, as required by representative claim 57.

CLAIMS 49 AND 62

Rather than arguing the rejections of claims 49 and 62 separately, the Appellants rely on the aforementioned arguments, which were unpersuasive. Therefore, we *conclude* that the Examiner did not err in finding that the combined teachings of Gafken, Arnold, Hasbun, Hayashi, Schmidt, and Menezes would have suggested the limitations of claims 49 and 62.

DECISION

We affirm the rejections of claims 49, 57, and 62, and of claims 44-48 and 58-61, which fall with claim 57.

No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1). *See* 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED

tkl

LENOVO (US) IP Law
1009 Think Place
Building One, 4th Floor 4B6
Morrisville NC 27560